BREXIT : Quid des données personnelles ?

Le Royaume-Uni a quitté l'Union européenne (UE) le 31 janvier 2020, mais une période transitoire est prévue jusqu'au 31 décembre 2020. Les britanniques restent donc soumis au règlement européen sur la protection des données personnelles (RGPD) jusqu'à cette date.
Par conséquent, à compter du 1e janvier 2021, **le Royaume-Uni sera considéré comme un pays tiers à l'UE et les transferts de données personnelles vers cet Etat seront strictement encadrés**. En cas de transferts illicites, la CNIL pourra appliquer les sanctions du RGPD (jusqu'à 4% du chiffre d'affaires ou 20 millions d'euros d'amende).

Qu'est-ce qu'un transfert de données personnelles ?

Un transfert de données personnelles est un **flux d'informations permettant d'identifier un individu** (nom, prénom, adresse électronique, téléphone, adresse postale, numéro de sécurité sociale, image, matricule professionnel…) **entre un Etat membre de l'UE et un pays tiers**.

Suis-je concerné par un transfert de données personnelles ?

Sans le savoir, une grande majorité des entreprises effectuent des transferts de données personnelles hors UE, du fait notamment des prestataires informatiques qu'ils utilisent, de leur présence sur les réseaux sociaux ou de la gestion de salariés expatriés.

Il est donc essentiel d'identifier les éventuels flux de données de votre entreprise et de vérifier le lieu d'implantation de certains de vos services informatiques ou la nationalité de vos cocontractants.

Quelles mesures dois-je mettre en place ?

- **Rien si un accord ou une décision d'adéquation est adopté(e)** : la Commission européenne doit vérifier que le Royaume-Uni offre un niveau suffisant de protection des données personnelles et, le cas échéant, elle peut adopter une décision d'adéquation. Cette dernière suffit à transférer des données personnelles sans formalités supplémentaires.
  Cette hypothèse est fortement compromise au regard du calendrier.

---

ou

- **Adopter des garanties appropriées pour continuer les transferts** : si aucune décision d'adéquation n'est adoptée (ce qui risque d'être le cas au regard du calendrier), les entreprises devront **prévoir des mesures supplémentaires pour garantir la protection des données** (le groupe des CNIL européennes travaillent actuellement sur la définition de telles mesures) **ET** :

  +

  - ***Adopter des règles d'entreprise contraignantes (ou Binding Corporate Rules / BCR)*** : ces règles s'adressent aux groupes d'entreprises qui transfèrent de façon régulière des données hors UE.
    Comment préparer un dossier BCR : https://www.cnil.fr/fr/comment-preparer-un-dossier-de-bcr ?
    Quelles sont les étapes de l'approbation des BCR par la CNIL :
    https://www.cnil.fr/sites/default/files/atoms/files/bcr-etapes_de_la_procedure_dapprobation.pdf

  ou - ***Faire signer au cocontractant (sans les modifier) des clauses contractuelles types telles que définies par la Commission européenne*** :
    https://www.cnil.fr/sites/default/files/typo/document/CCT-2010-Ss_Traitants_VF.pdf
    Guide pratique de la CNIL sur les clauses contractuelles types :
    https://www.cnil.fr/sites/default/files/typo/document/CNIL-transferts-CCT.pdf

---

ou

- **Arrêter les transferts de données et chercher une alternative** (par exemple en relocalisant les données en Europe, en changeant de prestataire, etc).